The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange
Policy Board Discussion Draft

Subject: Access	**Submission Date: 05/17/2010**
Implementation Date: TBD	**Scheduled Review Date: TBD**

Brief Definition: The access policy describes a participating provider's ability to obtain access to health information through the HIE.

Background and Purpose: Each user accessing the HIE will have a defined role. The access policy ensures that each user will only have access to information necessary to conduct activities associated with that role.

Responsibility: The HIE and its participating providers will have responsibilities related to access. The HIE will make this policy known through participant outreach and education and enforced through the participation agreement

Policy: CRISP will use role-based access to control access levels for each user in the HIE. CRISP will create a list of universal access roles based on the level of information necessary for care. Each participating provider organization will be responsible for assigning roles to users, as these organizations will be most familiar with the level of access needed to carry out job function.

Additionally, access to a patient's information will only be granted if the participating provider has an established treatment relationship with the patient (as determined by the registration process). The only exception to this is the break-the-glass function through which emergency users can access information only in the event of an emergency, and if the patient has not opted-out of the HIE.

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange
Policy Board Discussion Draft

Subject: Audit	**Submission Date: 05/17/2010**
Implementation Date: TBD	**Scheduled Review Date: TBD**

Brief Definition: The audit policy describes the HIE's procedures for auditing access to and use of the HIE.

Background and Purpose: The purpose of the audit policy is to provide ongoing monitoring of compliance with all applicable laws, regulations, and CRISP policies. The ability to execute periodic and ad hoc audits gives CRISP the ability to monitor participating providers' compliance with CRISP contractual requirements and, if detected in the course of such monitoring, violation of legal or regulatory requirements. If CRISP does find that a participating provider is in violation of its contract, CRISP will take prompt action to enforce the contract with the participating provider. CRISP is not responsible for nor obligated to monitor general legal or regulatory compliance by its participating providers. However, CRISP will take what it deems to be reasonable steps, typically notification of the participating provider, if such violations are detected during the course of an audit.

Responsibility: The HIE and its participating providers will have responsibilities related to audit. The HIE will make this policy known through participant outreach and education and enforced through the participation agreement.

Policy: CRISP will maintain an audit trail as a mechanism to demonstrate compliance with participant use and disclosure authorization(s). The audit trail will contain date-, time-, and source-stamped historical records of activities and transactions that pertain to HIE access and the use and disclosure of personal health information available through the HIE.

Each entry will be immutable (unchanging and unchangeable) in content. CRISP will maintain an active audit trail for the previous six months, with an archive of three years of audit information

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange
Policy Board Discussion Draft

Subject: User Authentication	**Submission Date: 05/17/2010**
Implementation Date: TBD	**Scheduled Review Date: TBD**

Brief Definition: The user authentication policy describes the conventions for establishing new users and passwords for access to the exchange.

Background and Purpose: Authentication assures the confidentiality of health information by requiring that the identities of all individual participants of the HIE are verified when accessing the HIE. This policy sets forth the actions required for participant authentication when attempting to access the statewide HIE and to establish standards for authentication.

Responsibility: The HIE and its participating providers will have responsibilities related to authentication. The HIE will make this policy known through participant outreach and education, and enforced through the participation agreement.

Policy: The CRISP HIE will utilize single-factor authentication (user name and strong password) for access to the HIE via Elysium EMR application and VHR. For users accessing via a third-party EMR, this user name and password will still be available for remote access, but will not be necessary to access the HIE from within the third-party EMR.

User Name Convention
User Names will consist of the first letter of the user's first name, and the user's full last name (or truncated version of the last name if its longer than XX characters). EXAMPLE (John Doe "JDoe").

If the user name of a new user is identical to that of an existing user, the second letter of the new user's first name will be inserted after the first letter. If after all the letters in a user's first name are utilized an identical user name still exists, then a number will be appended after the last name, starting with the number "1". EXAMPLE (Jane Doe "JaDoe", Johnny Doe "JoDoe", Jo Doe "JoDoe1")

Password Convention
Passwords must be at least eight (8) characters, contain three (3) of the four (4) character types (UPPER case letter, lower case letter, number, symbol); must not contain 4 consecutive characters that are consecutive in the user's username (user name: JDoe, password; JDoe1 not allowed); must not contain the name of the user's organization; must not contain the following

words/phrases “CRISP”, “HIE”, “password”; and must not be identical to any of the user’s previous passwords.
An encrypted record of all users’ previous passwords will be kept in order to ensure a user does not duplicate his previous passwords.

Authentication Attempts

Authentication must be provided at every access attempt. The HIE shall record all authentication access attempts. After five (5) consecutive failed log-in attempts a user will be locked out. The lock-out will be terminated only after the user’s identity is verified and his or her password is reset.

Password Changes
A user will be able to reset his or her password via the VHR portal.

A user will have to change his or her password every six months. Users will be reminded to change their password upon log into the VHR or Elysium EMR application, but not via third-party EMR. Access to the exchange via third-party EMR will not be affected by a user’s password status.

Authentication Data.
The HIE shall ensure authentication data is secure at the time it is entered and is administered safely. The HIE shall ensure the safety and identity of active and non-active participant user names and passwords.

Authentication Violation
HIE participants are responsible for reporting to the HIE participant individual suspected activity in violation of the HIE authentication policies or any participant individual activity that may cause harm to the HIE or its participants.

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange
Policy Board Discussion Draft

Subject: User Authorization	**Submission Date: 05/10/2010**
Implementation Date: TBD	**Scheduled Review Date: TBD**

Brief Definition: Upon individual participant authentication and access to the HIE, the HIE must verify which functions that a user is authorized to perform. The HIE shall assign participants access roles. Participants shall be authorized to access health information consistent only with the functions defined by the access roles.

Background and Purpose: Authorization assures the confidentiality of health information by requiring that the HIE verifies the access role a user is assigned. This policy sets forth the minimum requirements for authorized uses of the HIE.

Responsibility: The HIE and its participating providers will have responsibilities related to authorization. The HIE will make this policy known through participant outreach and education, and enforced through the participation agreement.

Policy: The HIE shall allow individual participants to access health information based upon the access role assigned to them by the HIE. At present, authorization of access to health information is limited to treatment, payment for treatment, and health care operations.

1. **Role-based Access.** The HIE will assign participants user access roles. Participants shall only be authorized to access the HIE in compliance with the assigned role definition.

2. **Creation and Management of Users:** CRISP will be responsible for the creation and management of users who access the HIE. User Authorization will be managed by ensuring that requests for new users come from participant verified "super-users" with the ability to submit new user requests. No user will be authorized to access the exchange unless the request to create that user originates from the participant's "super-user."

3. **Physician Address Book:** CRISP will be responsible for ensuring that all of the necessary user information is present for a complete entry into the physician address book or other user database.

4. **Unauthorized Access**. All access not consistent with the HIE policies shall be deemed unauthorized. Unauthorized access shall set forth immediate termination of access privileges and may be subject to other penalties by the HIE.